IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.: 09/977,351 Confirmation No. 3978

Applicant: Y. IKEDA

Filed: October 16, 2001

Title: INFORMATIONDISTRIBUTING SYSTEM AND METHOD THEREOF

TC/AU: 2134

Examiner: T. Ho

Customer No.: 24956

SUBMISSION OF CERTIFIED PRIORITY DOCUMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicants submit herewith a certified priority document of corresponding Japanese Patent Application No. 2000-316200, filed October 17, 2000 for the purpose of claiming foreign priority under 35 U.S.C. § 119.

Applicants respectfully request that the priority document be submitted and filed and officially considered of record.

Respectfully submitted,

John R. Mattingly
Registration No. 30,293
Attorney for Applicant

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.
1800 Diagonal Road, Suite 370
Alexandria, Virginia 22314
(703) 684-1120
Date: October 31, 2005

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日
Date of Application: ２０００年１０月１７日

出 願 番 号
Application Number: 特願２０００－３１６２００

出 願 人
Applicant(s): 株式会社日立製作所

09/977,351
NIT-307
Mattingly Stanger Malur
703 684-1120

２００１年１０月１９日

特 許 庁 長 官
Commissioner,
Japan Patent Office 及川耕造

【書類名】　特許願
【整理番号】　NT00P0535
【提出日】　平成12年10月17日
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 15/16
【発明者】
【住所又は居所】　神奈川県秦野市堀山下１番地　株式会社日立製作所　エンタープライズサーバ事業部内
【氏名】　池田　圭伸
【特許出願人】
【識別番号】　000005108
【氏名又は名称】　株式会社日立製作所
【代理人】
【識別番号】　100068504
【弁理士】
【氏名又は名称】　小川　勝男
【電話番号】　03-3661-0071
【選任した代理人】
【識別番号】　100086656
【弁理士】
【氏名又は名称】　田中　恭助
【電話番号】　03-3661-0071
【選任した代理人】
【識別番号】　100094352
【弁理士】
【氏名又は名称】　佐々木　孝
【電話番号】　03-3661-0071
【手数料の表示】
【予納台帳番号】　081423

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】情報提供装置および方法

【特許請求の範囲】

【請求項１】

Ｗｅｂサーバと、インタネットに接続され前記Ｗｅｂサーバの配信する情報の複製を保持しユーザからの要求に応じて前記情報の配信を行なう複製Ｗｅｂサーバと、前記Ｗｅｂサーバと前記複製Ｗｅｂサーバの間に設置されあらかじめ定められたプロトコルを用いたもので且つ、前記複製Ｗｅｂサーバからの接続要求であるときのみ接続を許可するファイアウォールとを備えたことを特徴とする情報提供装置。

【請求項２】

前記Ｗｅｂサーバは前記ファイアウォールを通した接続要求が許可された接続相手からのものかどうか判断し、そうでなければ通信を切断し、そうであれば要求されたデータを前記ファイアウォールを通して接続要求を出した前記複製Ｗｅｂサーバへ送信することを特徴とする請求項１記載の情報提供装置。

【請求項３】

Ｗｅｂサーバと、インタネットに接続され前記Ｗｅｂサーバの配信する情報の複製を保持し、ユーザからの要求にしたがって保持する情報を提供する複数の複製Ｗｅｂサーバと、前記Ｗｅｂサーバと前記複数の複製Ｗｅｂサーバの間に設けられたファイアウォールとを有し、前記複数の複製Ｗｅｂサーバは互いに保持する情報が一致しているかどうかを判定することを特徴とする情報提供装置。

【請求項４】

前記互いに保持する情報が一致しているかどうかの判定はそれぞれの保持する情報の検査コードを比較することにより行なわれることを特徴とする請求項３記載の情報提供装置。

【請求項５】

更に、複数の前記複製Ｗｅｂサーバへのユーザ端末からの接続要求を前記複数の複製Ｗｅｂサーバに分散せしめる負荷分散装置を備えたことを特徴とする請求項３記載の情報提供装置。

【請求項６】

Ｗｅｂサーバと、インタネットに接続され前記Ｗｅｂサーバの配信する情報の複製を保持し、ユーザからの要求にしたがって保持する情報を提供する複数の複製Ｗｅｂサーバと、前記Ｗｅｂサーバと前記複数のＷｅｂサーバとの間で通信を行なわせる専用接続線を備えたことを特徴とする情報提供装置。

【請求項７】

配信される情報を記憶する情報処理装置と、インタネットに接続され配信される情報の複製を記憶し、要求に従い情報の複製を配信する複数の情報配信装置とを有する情報提供装置における方法であって、前記情報処理装置が保持する情報の一部又は全てを前記情報配信装置の一つ又は複数に転送するステップと、複数の前記情報配信装置が保持する情報を互いに比較するステップとを有することを特徴とする情報提供方法。

【請求項８】

配信される情報を記憶する情報処理装置と、インタネットに接続され配信される情報の複製を記憶する複数の複製Ｗｅｂサーバとを有する情報提供装置における方法であって、ある複製Ｗｅｂサーバから他の複製Ｗｅｂサーバの指定する情報の一致をチェックする場合において、他の複製Ｗｅｂサーバにおいて指定された情報があるかどうかを調べ、あるときはその情報の検査コードを前記あるＷｅｂサーバに転送し、前記あるＷｅｂサーバにおいて、前記指定された情報に対応する自サーバが記憶するファイルの情報の検査コードを求め、これら２つの検査コードを比較し、一致するときはチェックを終了し、一致しないときは前記情報処理装置から対応する情報を入手して保存することを特徴とする情報提供方法。

【請求項９】

前記他のＷｅｂサーバにおいて指定された情報がないとき前記情報処理装置から当該情報を入手し保存すると共に検査コードを前記あるＷｅｂサーバに転送することを特徴とする請求項８記載の情報提供方法。

【請求項１０】

前記情報処理装置にも指定された情報がない場合に前記あるＷｅｂサーバの当該情報を削除することを特徴とする請求項９記載の情報提供方法。

【請求項１１】

配信される情報を記憶する情報処理装置と、インタネットに接続され配信される情報の複製を記憶し、要求に従い情報の複製を配信する複数の情報配信装置とを有する情報提供装置における方法であって、前記情報配信装置が配信する情報に付加された電子署名により、情報の正当性を評価することを特徴とする情報提供方法。

【請求項１２】

前記電子署名の有無、または電子署名の数により、前記情報配信装置が配信する情報の配信先の範囲を制御することを特徴とする請求項１１記載の情報提供方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、インタネットに接続された情報処理システムに対し、システム内外からの不正な改ざんからシステムに登録されている情報を防護する方法および防護を施した装置に関する。

【０００２】

【従来の技術】

近年インタネットの普及により、多くの相互接続されたコンピュータ機器が様々な用途で利用されている。このようなコンピュータ機器に対し不正なアクセスからシステムを防護する手段として、次のような方式が実用化されている。図１は最も代表的な防護例である。ファイアウォール（防火壁）と呼ばれるシステムをインタネットと情報処理システムの途中に接続し、ここで不正なアクセスの振るい落としをすることによってインタネット側に対して提供するサービスを制限している。また、図２のようにサービスを提供するコンピュータ機器をファイアウォールの外側に置き、コンピュータ機器側で何らかの防護策を取る場合もある。

【０００３】

特開平１１－２６６２７９号公報の記載では、図２に示すシステムのようにフ

ァイアウォールの外部にメールサーバを設置することで、ファイアウォール外部のユーザがファイアウォールを介さずにメールの送受信を行うことを可能とし、ファイアウォール内のネットワークのセキュリティを高めている。

【０００４】

【発明が解決しようとする課題】

従来の防護システムは、ファイアウォールと呼ばれるシステムに頼った形となり、外からの攻撃に対する強さはファイアウォールの強さに依存してしまう問題があった。また、ファイアウォールは一般に高価な導入コストと管理コストを必要とする。

【０００５】

また、インタネットに対して様々なサービスを提供するにあたって、それに応じた情報処理システムに対する様々な機能追加が必要になるが、これらの機能追加によりファイアウォールの内部構造は複雑化してしまい、性能の劣化や新たなセキュリティホールを産み出す要因になってしまう。

【０００６】

更に、サービス提供機器をファイアーウォールの外側に置いた場合、攻撃に対する防御の必要性からサービスを提供する機器に対してファイアウォールの内側から容易に入ることができない。

【０００７】

また、一般的なファイアウォールでは外部からの攻撃には耐えられるが、内部からの不正な改ざんに対しては配慮がなされておらず、効力を持たない。

【０００８】

従来のシステムでは情報処理システムの情報に不正な改ざんがあった場合に対して発見が容易でなく、不正な侵入への常時監視に対し高い費用が発生する。

【０００９】

従来のプロクシサーバは、外部インタネットへの代理接続（WWW閲覧ソフトを実行しているユーザのコンピュータの代理としてユーザの要求するWWWサーバに接続を試み、そして、接続が成功した場合、そのWWWサーバから取得できたデータをユーザに送信すること）や一次保存（WWWサーバから取得できたデ

ータをユーザに送信するとともに、同一データの要求に備えて自らの記憶領域に一時的に保存すること）を目的とするものであり、外部向けサービス提供機器を保護する用途として内部インタネットへの接続を代行するものではない。また、従来のミラーサーバは、ミラー対象サーバの内容を複写し、システム及びネットワーク的な負荷分散を目的とし、防護システムに対する特別な配慮はない。これらのように、従来のミラーサーバやプロクシサーバの場合、セキュリティに於ける配慮は従来の防護システムと何ら変わらず、本質的に解決されない。

【００１０】

本発明の目的は、インタネットに対してサービスを提供する機器に対し、不正な改ざんに強く監視が容易なシステムを提供し、システムの運用コストを低減することである。

【００１１】

【課題を解決するための手段】

上記目的を達成するため本発明では、ファイアウォールの内側にあるサービス提供システムのレプリカ（複製）をファイアーウォールの外側に複数置き、利用者はこれらレプリカからのみサービスの提供を受けるようにする。サービス提供者はファイアーウォールの内側にある本来のサービス提供システムに対し、情報を登録する。このシステムはファイアウォールの内側であるので、セキュリティホールをあまり気にせずに様々な手段で情報を登録することができる。

【００１２】

複数のレプリカは本来のサービス提供システムの情報を常に複写しておくようにする。レプリカは定期的にレプリカ同士が保持する情報の内容を互いに比較することにより、不正な改ざんが発生したかどうかのチェックを行う。ここでレプリカの保持する情報の間に差異がある場合はファイアウォールの内側にある本来のサービス提供システムから本来あるべきデータがレプリカに対し複写され、レプリカによって不正な改ざんがあったかどうかを検査し、元の情報に修正し、管理者に通報することができる。

【００１３】

レプリカに複写される情報には電子署名を付加することができる。この機能を

使用する場合、レプリカは利用者に情報を発信するにあたって電子署名が有効であるかどうかを検査し、有効である場合は発信し、無効である場合は管理者に連絡する（レプリカがWWWサーバに無効であることを連絡の後、WWWサーバが管理者にメールやＳＮＭＰメッセージ等で連絡する）。これにより、必要な電子署名を付加する権限のない者が情報の公開や改変行為を行うことをできなくすることができる。

【００１４】

複数のレプリカは互いにサービスを行なうサーバとして入れ替わることにより、インタネット側からは同一の機器に見せる。このことにより、内部的に不正な接続のあった装置とそうでない装置を分け、それらを互いに比較しあうことができる。また、サービスを提供するレプリカの負荷を分散し、速度の低下を防ぐことができる。

【００１５】

【発明の実施の形態】

図３は本発明を、WWWサービスを提供するシステムの実施の形態としてブロック図で示したものである。図３において、インタネット１から見えるレプリカ８は４台、WWWサーバ３は１台しか示されていないが、実際にはこれ以上の台数が接続されていたり、１台の機械を論理的に複数台に見立てている場合も考えられる。また、このレプリカ８は多段に接続することもできる。さらに、このレプリカ８はインタネット上の他の場所にあっても良く、レプリカ８の配置次第ではネットワークの負荷分散をすることができる。

【００１６】

登録情報作成者は登録情報作成システム４からWWWサーバ３に情報を登録する。WWWサーバ３はファイアウォール２で防護されている為、この時用いられる手段は、一般に用いられるネットワーク転送手順の何れでも良い。これは、例えばWWWサーバ３をファイルサーバに見立て、WWWサーバ３とＰＣなどで構成される登録情報作成システム４間でファイル共有を行うことで実現できる。

【００１７】

図１０を用いてレプリカ８、ファイアウォール２、WWWサーバ３の間の通信

について説明する。レプリカ８はファイアウォール２を介してWWWサーバ３と通信を行うが、この際ファイアウォール２はＨＴＴＰ用のポートのみを外部ネットワークに対し開放している。もし外部ネットワークからの通信が、ＨＴＴＰ以外のポートに対するものであれば（１００１　Ｎｏ）、ファイアウォール２はこの通信を切断する。外部ネットワークからの通信がＨＴＴＰ用のポートに対するものであるなら（１００１Ｙｅｓ）、ファイアウォールは次にこの通信の発信元を、パケットのヘッダ中の情報から識別し、レプリカ８からの接続要求かを判断する（１００２）。パケットの発信元が外部ネットワークに設置されたレプリカ８であれば接続を許可するが、それ以外の機器が発信元である場合は、通信を切断する。もしＨＴＴＰにより接続要求をしている機器がレプリカ８であるなら、ファイアウォール２はレプリカ８に対し接続を許可し、接続許可の応答をファイアウォール２より受けたレプリカ８はコマンドの作成（１００３）及び送信を行い、WWWサーバ３に対し処理を要求する。レプリカ８からのコマンドをWWWサーバ３に仲介するファイアウォール２では、コマンドの文法チェックを行い（１００４）、文法に誤りがある場合には通信を切断する。チェックの結果文法が正しい場合は、ファイアウォール２はWWWサーバ３に対しＨＴＴＰによる接続要求を行う。WWWサーバ３は、接続要求の発信元を識別し（１００５）、それが許可された機器であれば接続許可の応答を返信するが、そうでなければ通信の切断を行う。接続許可の応答を受けたファイアウォール２は、レプリカ８から送信されたコマンドをWWWサーバ３へ送信する。ファイアウォール２からのコマンドを受けたWWWサーバ３は、コマンドにより要求された処理に応じてデータを作成し（１００６）、このデータをファイアウォール２に送信する。ファイアウォール２はこのデータをレプリカ８に送信し、さらにレプリカ８に対して新たなコマンドの受け付けを行う。引き続きレプリカ８がWWWサーバ３に処理を要求するなら（１００７　Ｎｏ）、レプリカ８におけるコマンド作成以後の処理を繰り返すが、WWWサーバ３に対する要求が無いのであれば、レプリカ８はファイアウォール２に対し通信を切断する要求を送信し、ファイアウォール２からはWWWサーバ３に対し同様に通信を切断する要求を送信することでレプリカ８、ファイアウォール２、WWWサーバ３の間の通信を切断して一連の処理を終了す

る。

【００１８】

上記のようにファイアウォールはレプリカからのＨＴＴＰを用いた接続要求のみを受け付けるため、市販の高価なファイアウォールシステムを用いなくとも、ＨＴＴＰプロクシ（代理）サーバをフリーソフトウェアを用いて安価に構築し、ファイアウォールとして利用することも可能である。

【００１９】

勿論、顧客が既に導入しているファイアウォールやＷＷＷサーバをそのまま利用することも可能であり、この場合顧客はレプリカ８を新規導入し、ＷＷＷサーバ上に追加の設定(レプリカの複写、更新の機能の追加)を実施してＷＷＷサーバ３とする。レプリカ８はこれらの機構を通して、ＷＷＷサーバ３の複製となる。このように一般的なＨＴＴＰ接続のみを用いてレプリカ８はＷＷＷサーバ３の複製となるので、レプリカ８はＷＷＷサーバ３の内容を書き換えることが出来ない。

【００２０】

レプリカ８はインターネット１上のユーザ端末に対し、所定のポートに対する接続及び通信のみを許可する。このとき、この接続を待つ以外のポートは使用せず、ユーザ端末が接続できないようにする。ネームサーバ９は登録されているエントリを随時変更し、同一のレプリカにアクセスが集中しないようにする。例えば図１１に示すように、ユーザ端末がｗｗｗ．ｊａｐａｎ．ｃｏ．ｊｐのドメインネームを持つＷＷＷサーバへの接続要求を行うと、ネームサーバはこのＷＷＷサーバの複製であるレプリカに与えられたＩＰアドレス（１）～（４）のうちの1つを、ラウンドロビン方式で、もしくはランダムに返信する。ユーザはこのネームサーバが返信したＩＰアドレスに対し接続を行うため、図１１に示す４つのレプリカの間でユーザからのアクセスが分散されるために1つのレプリカに対しアクセスが集中することを回避することができる。

【００２１】

これは図５のようにスイッチ１０を用い、レプリカ８への通信経路を切り替えることで実現することもできる。レプリカ８とファイアウォール２を、図４や図

５のようにインタネット１とは別のネットワークを経由して接続し、ファイアウォール２をインタネット１からネットワーク的に分離すれば、システムとしての防護性能を更に上げることができる。以上のことからネームサーバ９やスイッチ１０は負荷分散装置として機能する。

【００２２】

また図６のように、レプリカ８及びスイッチ１０を1つの機器であるＷＷＷセキュリティ装置１１として構築し、専用ケーブル等の一般的なネットワーク以外の手段を用いＷＷＷサーバ３と直接接続することで、防護性能を保ったままファイアウォール２を省略することもできる。ＷＷＷセキュリティ装置１１はインタネット１からの接続要求をスイッチ１０で分散し、複数のレプリカ８に分配する。このレプリカ８は論理的に複数台とする構成でも良いし、スイッチ１０を使わず図３や図１１で説明したようなネームサーバを用いて振り分けても良い。

【００２３】

レプリカ８はインターネット１上に存在するユーザ端末からの接続要求を所定のポートで受けると、自らが保持しているＷＷＷサーバ３の情報の複製をユーザ端末に送信する。図９を用いて、レプリカ８が、ユーザ端末が要求する情報を配信する処理を説明する。

【００２４】

ユーザ端末はＧＥＴコマンドを用いて／ｈｏｇｅ／ｉｎｄｅｘ．ｈｔｍｌというファイルをレプリカ８に要求するが、レプリカ８がこのファイルの複製を保持している場合は（９０１　有）、ＷＷＷサーバ３に対しアクセスは行わない。レプリカ８が保持するファイルに後述する電子署名が付加されている場合はその電子署名のチェックを行い（９０３）、電子署名が適正なものであれば（９０３　ＯＫ）ユーザに／ｈｏｇｅ／ｉｎｄｅｘ．ｈｔｍｌファイルを送信し、電子署名に誤りがあれば（９０３　ＮＧ）ＷＷＷサーバ３にエラーを通知しまたユーザに対しても該当するファイルが存在しない旨をエラー通知する。この電子署名のチェックはオプションであり、電子署名を用いない場合はこの処理を行わずにファイルをユーザ端末に送信する。レプリカ８が／ｈｏｇｅ／ｉｎｄｅｘ．ｈｔｍｌファイルを保持していない場合は（９０１　無）、図１０に示した処理を経てレ

プリカ８とWWWサーバ３間で接続を確立した後、WWWサーバ３に対しコマンドを送信して／ｈｏｇｅ／ｉｎｄｅｘ．ｈｔｍｌファイルの送信を要求する（新規複写）。WWWサーバ３はファイルを保持している場合（９０２　有）はレプリカ８にそのファイルを送信し、レプリカ８は送信されたファイルに電子署名が付加されていればそのチェックを行い、そしてファイルをユーザに送信する。WWWサーバ３がファイルを保持していない場合（９０２　無）は、WWWサーバ３からレプリカ８ならびにユーザ端末に対してエラーを通知する。

【００２５】

基本的には上述のように、新規複写はユーザの要求があったページがレプリカ８上に存在しない場合にWWWサーバ３からその情報を取得することにより行い、一方、WWWサーバ３が保持する最新の情報をレプリカ８が保持する同じ情報に反映する処理（更新）は、レプリカ８とWWWサーバ３とのコンペアチェックの結果によって行うことができる。これは、以下の手順で予め用意しておくこともできる。

【００２６】

図９の更新の場合、レプリカ８はWWWサーバ３もしくはカスケード接続された上位のレプリカ８に接続を行う（９０４）。そして該当の情報についてＣＲＣのエラーチェックコードの計算を行なう（９０５）。一方、WWWサーバ３では求められたファイルが存在するかどうかを判定し（９０２）、なければ（９０２　無）、エラー情報をレプリカ８へ送る。レプリカ８ではこれを受けて当該ファイルを削除する（９０７）。該当するファイルがあれば（９０６　有）、同様にその情報についてＣＲＣのエラーチェックコードを計算し、作成する（９０８）。これを更新日付と共にレプリカ８に転送する。次に、レプリカで計算され求められたＣＲＣとWWWサーバから転送されたＣＲＣとを比較し一致するかどうか調べる（９０９）。一致すれば、情報の更新はなかったことを意味しレプリカ８の情報の更新はしない（９１０）。一致しなければ、レプリカ８はWWWサーバにファイルの転送を要求し、これを保存する（９１１）。

【００２７】

以上の処理はインタネット上のユーザとのやり取りは遮断し、レプリカ８とW

ＷＷサーバ３の間だけで実行される。

【００２８】

即時更新のときは、レプリカ８はＧＥＴコマンドで更新情報の要求を出す（９１２）。ＷＷＷサーバ３は情報の更新が生じるまでこの要求を保留しておき、更新が発生した時点で更新情報を応答として返す。これを用いることにより、ＷＷＷサーバ３の更新後即時にレプリカ８を更新することができる。

【００２９】

レプリカ８はＷＷＷサーバ３の全てのコンテンツに対する複製を保持するのが基本であるが、設定により保持する複製の量や複製する場所を設定できる。すなわち、サーバ上のコンテンツが複数のディレクトリやファイルから構成される場合、どこからどこまでのディレクトリやファイルを複製の対象とするかを指定できる。さらに、複製の対象とするファイルの数やサイズに制限を設けるよう指定することができる。これによって、例えば、ディレクトリ毎に複製するファイルの数や全体サイズを制限したり、大きなファイルの複製制限等の制御ができる。また、複製する対象を容量やアクセス頻度等に応じて自動的に選択し、動的に変化させることができる。

【００３０】

外部ネットワークに複数設置されたレプリカ８には、ネットワーク上のユーザによる不正な改ざん行為に対する防衛手段が施されていないため、レプリカ８同士や内部ネットワーク上のＷＷＷサーバ３との間で定期的にコンペアチェックを行い不正な改ざんを発見し、レプリカ８が保持し配信する情報の信憑性を保つ。

【００３１】

図８を用い、１台目のレプリカ８（装置Ａ）が保持する／ｆｏｏ／ｉｎｄｅｘ．ｈｔｍｌファイルのコンペアチェックの処理を説明する。まず、装置Ａは２台目のレプリカ８（装置Ｂ）に対し、ＨＴＴＰプロトコルの“ＨＥＡＤ　／ｆｏｏ／ｉｎｄｅｘ．ｈｔｍｌ”コマンドにより、装置Ｂが保持する／ｆｏｏ／ｉｎｄｅｘ．ｈｔｍｌファイルの属性情報の送信を要求しコンペアチェックを開始する（８０１）。装置Ｂでは当該ファイルがあるかを調べ（８０２）、有る場合には当該ファイルのＣＲＣ計算を行なう（８０３）。そしてそれを更新日付と共に装

置Ａに送る。一方、装置Ａでも当該ファイルのＣＲＣ計算を行ない（８０４）、装置Ｂから転送されたＣＲＣと一致するかどうか判定する（８０５）。一致すれば、不正な改ざんがなかったとしてチェック終了する（８０６）。

【００３２】

また、装置ＡからＨＥＡＤコマンドを受けた装置Ｂが要求されたファイルを保持していない場合（８０２　無）、装置ＢはＨＥＡＤコマンドの応答を装置Ａに返す前にＷＷＷサーバ３にＧＥＴコマンドで接続しファイルの送信要求を行う。ＷＷＷサーバ３に当該ファイルがあれば（８０７　有）、当該ファイルを取得して保存し（８０８）、同様にＣＲＣ計算を行なう（８０９）。

【００３３】

これは、装置ＡのＣＲＣと比較され一致すればチェック終了し（８０６）、一致しなければ改ざんなどにより装置Ａのファイルが正しくないとしてＷＷＷサーバ３から取得したファイルを装置Ａに保存する（８１０）。

【００３４】

ＷＷＷサーバ３が要求されたファイルを保持していない場合そのファイルは、ＷＷＷサーバ３から削除されたか、ネットワーク上の侵入者により装置Ａに対し勝手に追加されたファイルだと解釈される。そこで装置ＢはＨＥＡＤコマンドの応答として装置Ａに該当ファイルの削除命令を返し、ＷＷＷサーバ３には新たな属性を加えたＨＥＡＤコマンドで削除命令発行の旨を通知する。装置Ａは削除命令を受けた後、実際にそのファイルを削除し、削除完了の旨を新たな属性を加えたＨＥＡＤコマンドでＷＷＷサーバ３に通知する。これは、削除せず別の記憶領域に一時保管したり、ＰＯＳＴコマンドでＷＷＷサーバ３の特定記憶領域に保管することもでき、これにより不正アクセスであった場合に証拠を残すことができる。これらの応答は互いに暗号を用いることもでき、ネットワーク的に遠隔なレプリカに対しても安全に削除情報を送ることができる。以上のようにコンペアチェックは実施されるが、レプリカ８とＷＷＷサーバ３との間が独自手順で実装されている場合、ＨＥＡＤ、ＧＥＴ、ＰＯＳＴ各コマンドの仕様に縛られない、更に自由度のある設計をすることができる。

【００３５】

そしてレプリカ８は必要に応じて他のファイルに対し同様にコンペアチェックを行う。

【００３６】

コンペアチェックはレプリカ８同士のみではなく、レプリカ８とＷＷＷサーバ３との間で行うことも出来る。ＷＷＷサーバ３ではファイルの更新が行われる可能性があるため、ＷＷＷサーバ３を相手にコンペアチェックを行う場合は、レプリカ８が保持する情報が最新の内容であるか、情報の更新チェックを同時に行うことにもなる（図９における更新）。

【００３７】

ＨＥＡＤコマンドには新たな属性を加え（ファイルの日付やサイズ等を返す機能に加え検査用コードも返すように機能拡張する）、ファイルの検査コード（チェックサムやＣＲＣコード等）を得られるようにしておく。

【００３８】

ＨＥＡＤコマンドで取得した他装置又はＷＷＷサーバが持つ属性情報は、それを用いて比較を行うことが目的であるため、送受信するデータはハッシュ等により非可逆的に暗号化されていても良い。

【００３９】

ＷＷＷサーバ３に登録する情報は前述のように、登録時に署名生成手続きにより電子署名を行うことができる。電子署名を使用する場合の流れを図１２に示す。レプリカ８において、ＧＥＴコマンドによって要求されたファイルを準備する（１２０１）。次に、電子署名があるかどうかを調べ（１２０２）、ないときはこれはユーザには送信できないファイルと判断されるから、ユーザにはエラー、ファイル無しとの応答がなされる。署名があった時、この署名を評価する（１２０３）。そして対象ユーザ毎に配信可のものか、配信否のものかを判断する（１２０４）。送信可のユーザにはデータ送信をし、送信否のユーザにはエラー、ファイル無しとの応答がなされる。

【００４０】

図示してないが配信情報中の電子署名が正当な署名でない場合、レプリカ８はＷＷＷサーバ３が保持する情報を再複製し、その署名を検査することもできる。

このとき、再複製の情報も正当でない場合、利用者にはエラーの旨を配信する。いずれの段階でも管理者に対し不正署名の旨を通報することができる。

【００４１】

また、電子署名の利用により、図７のように配信情報をグループ分けし、配信先の制御を行うことができる。図７においては例として、情報に対しＡ、Ｂ、Ｃ、Ｄの４種の電子署名が付加され得る。ここで、４種全ての電子署名が付加された情報１は、社内および関連会社を含む社外にまで配信される情報として識別される。Ｂ、Ｃ、Ｄの３種の電子署名が付加された情報２は、社内および関連会社内までを情報配信の範囲として識別される。以下、情報３、情報４そして情報５と付加する電子署名の種類に応じてその情報の配信範囲を設定することが可能である。

【００４２】

この処理を示したものが図１３である。データの配信要求（１３０１）を受けたレプリカ８もしくはＷＥＢサーバ３は、まずユーザのＩＰアドレスが社内もしくは社外どちらのものであるかを識別する（１３０２）。ユーザのＩＰアドレスが社内のものであった場合は、さらに同じ部署のものかを識別する（１３０３）。もし同じ部署のものであれば（ユーザＣ）、電子署名のチェックは行わずに情報の配信を行う（１３０４）。ユーザのＩＰアドレスが他部署のものであった場合（ユーザＢ）は、ファイルを準備すると共に（１３０５）、配信する情報に付加された電子署名が他部署に対する情報配信を許可する種類のものであるかをチェックし（１３０６）、許可するものであれば配信を行いそうでなければユーザにエラー通知を行う。ユーザのＩＰアドレスが社外のものであった場合（ユーザＡ）は、ファイルを準備すると共に（１３０８）、配信する情報に付加された電子署名が社外に対して配信することを許可する種類のものであるかをチェックし（１３０９）、そうであれば配信しそれ以外のものであればユーザにエラーを通知し、その情報の配信は行わない。

【００４３】

以上のような電子署名の利用法は、従来社内向けと社外向け等のようにＷＷＷサーバ３を用途別に分けていた場合に有効で、電子署名の違いや有無により、配

信先を分別することができる。例えば、電子署名が無い情報はレプリカ８には複写されないか、複写されても配信できないので、ＷＷＷサーバ３に直接アクセス可能な場所からのみアクセス可能となる。これにより、社外向け情報は電子署名付、社内向け情報は電子署名無しと区別することにより、配信情報を社外／社内向けというようにグループ分けができる。また、電子署名の評価にあたって、署名内に記された情報により、特定の顧客のみの配信等の制御をすることもできる。

【００４４】

レプリカ８は基本的にＷＷＷサーバ３が配信する情報の複製作成機器であり、一度複製元の設定をしてしまえば大きな変更がない限りオペレータによる操作の必要はない。複製元の設定とはどのＷＷＷサーバ３をどれだけ複製するか、検査コードを使用するか、電子署名や暗号を使用するか、即時更新するかどうかの複製のポリシーなどを指す。

【００４５】

ファイアウォール２は通過させた情報について発信元等の属性情報を累積するが、この累積された属性情報はＷＷＷサーバ３で収集可能であるので、レプリカ８と同様に、オペレータによるファイアウォール２への操作の必要はない。このように、レプリカ８とファイアウォール２は運用される時点では人手を介した操作を必要としないので、このレプリカ８とファイアウォール２を物理的に隔離した部屋に置き、物理的な鍵をかけることができる。このことにより物理的な鍵を持たない、システム内部の者による不正なシステム侵入、情報公開や改変行為を防ぐことができる。

【００４６】

レプリカ８とＷＷＷサーバ３の間は一般的なネットワーク手順で接続する必要は無いので、ＷＷＷサーバ３側に通信機構を増設し独自の通信手順で接続するようにすれば、インタネットプロトコルを使用しないので、ファイアウォール２の必要がなくなる。これはシステム全体のコストダウンに寄与することができ、ファイアウォール２上のセキュリティ欠陥が原因でのシステム不正侵入やシステムダウン等を防ぐことができる。この独自手順での接続は、図６のように装置１１

として実装しなくとも、図４や図５の構成で実施することも可能である。装置１１は、レプリカ８とＷＷＷサーバ３との通信に独自手順を使用しない場合、ファイアウォール２を内蔵してしまっても良い。また、装置１１はルータ等、他のネットワーク装置の内蔵オプションとして実装しても良いし、ＷＷＷサーバ３に装置１１を内蔵しても良い。これらのように装置として本発明のシステムを実装した場合、システム構築や管理か簡便になるという利点がある。

【００４７】

以上、本発明の実施の形態を説明したが、レプリカ８を多段接続し、後段のレプリカ８は前段からの接続のみ受け付けるようにすれば、さらに防護性能を上げることができる。この場合、前段となるレプリカ８はインタネット１上の他の場所にあっても良く、利用者の多いネットワークに近い場所に設置すれば、全体のネットワーク負荷を軽減することができる。

【００４８】

【発明の効果】

インタネットを用いた情報発信システムにおいて、情報登録を容易にし、負荷を軽減し、不正な情報の登録や改ざんの検知が容易となり、改ざんされた場合でも元情報への訂正も容易にできる為、システムの構成および管理の手間と費用を大幅に改善できる。

【図面の簡単な説明】

【図１】

従来の技術を示すシステム構成図。

【図２】

他の従来の技術を示す構成図。

【図３】

本発明の実施の形態を示す概略システム構成図。

【図４】

図３に対し、ファイアウォールを隠して防護性を良くしたシステム構成図。

【図５】

図４に対し、スイッチを利用して更に防護性を良くし負荷分散性能も良くした

システム構成図。

【図６】

図５のシステムを装置として実装した場合の例を示す図。

【図７】

電子署名の評価による配信制御を示す図。

【図８】

コンペアチェックの構成例を示す図。

【図９】

即時更新機能の構成例を示す図。

【図１０】

ファイアウォールの構成例を示す図。

【図１１】

ネームサーバの構成例を示す図。

【図１２】

電子署名を用いた情報発信制御を示すフローチャート。

【図１３】

複数の電子署名を用いた情報発信制御を示すフローチャート。

【符号の説明】

１　インタネット

２　ファイアウォール（防火壁）

３　ＷＷＷサーバ

４　登録情報作成システム

５　ルータで保護された登録情報作成システム

８　レプリカ

９　ネームサーバ

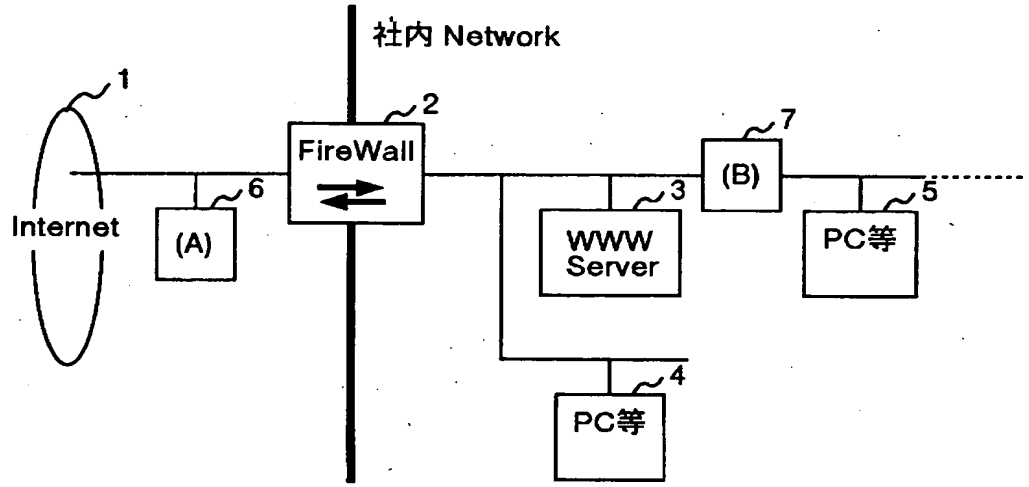
１０　負荷分散スイッチ

１１　ＷＷＷセキュリティ装置

【書類名】　図面

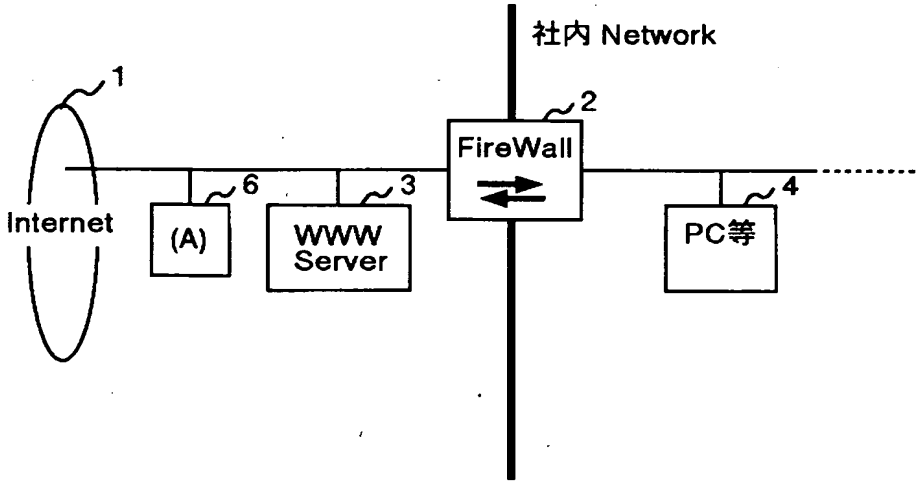
【図１】

図　1



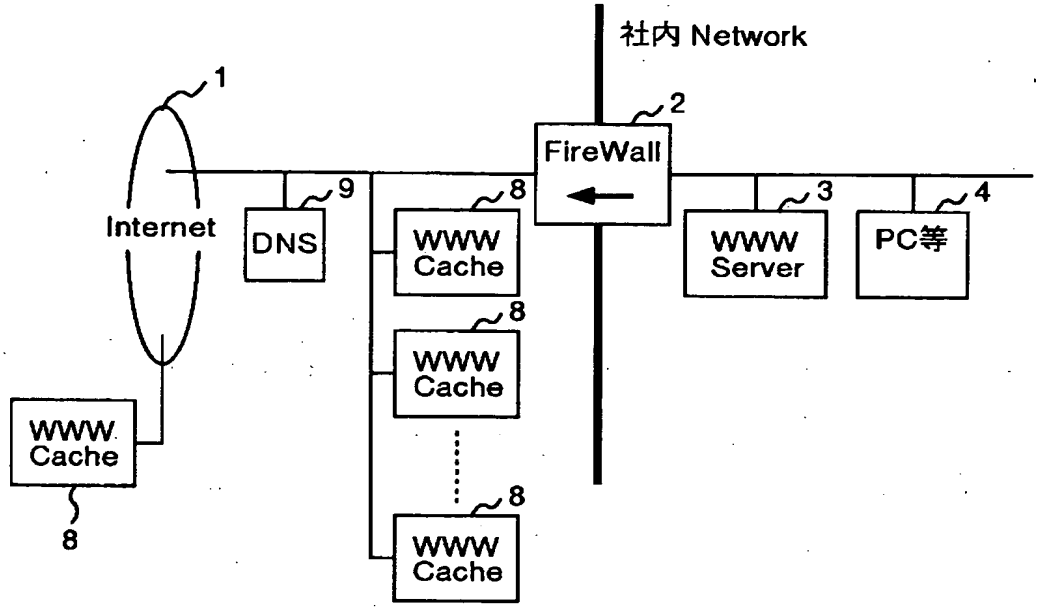
【図２】

図　2



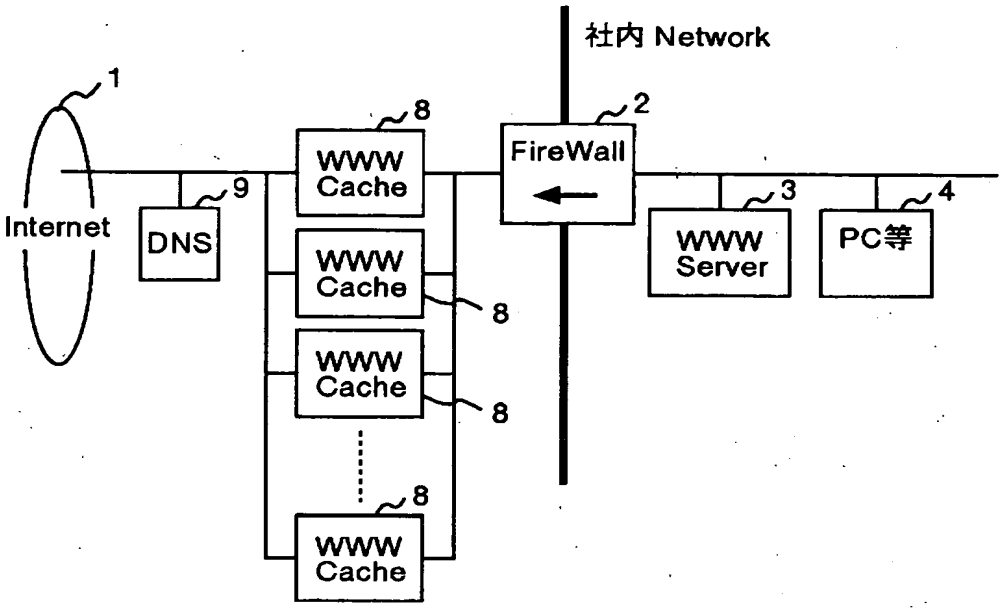
【図３】

図　3


社内 Network
1
2
FireWall
Internet
9
DNS
8
WWW
Cache
3
WWW
Server
4
PC等
8
WWW
Cache
8
WWW
Cache
WWW
Cache
8
8

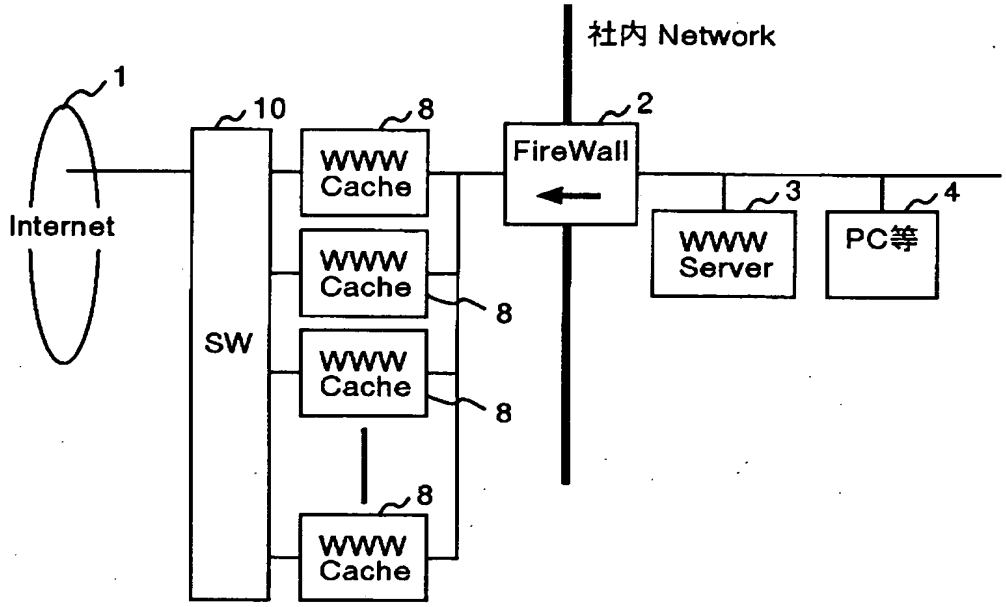
【図４】

図　4


社内 Network
1
Internet
DNS
9
8
WWW Cache
WWW Cache
8
WWW Cache
8
8
WWW Cache
2
FireWall
3
WWW Server
4
PC等

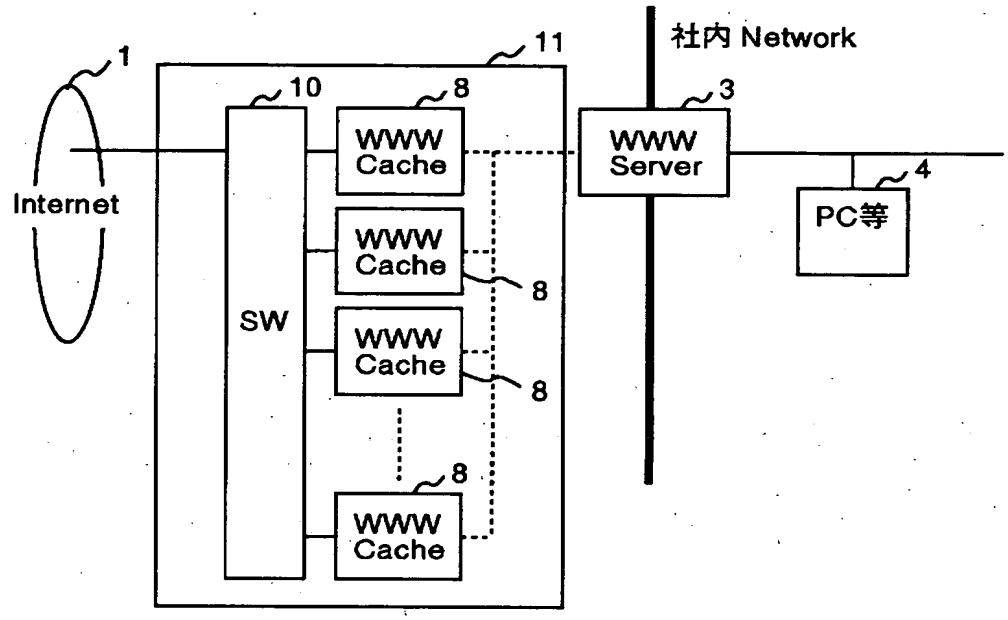
【図５】

図　5


社内 Network
1
10
8
2
Internet
SW
WWW Cache
WWW Cache
WWW Cache
WWW Cache
FireWall
3
4
WWW Server
PC等
8
8
8

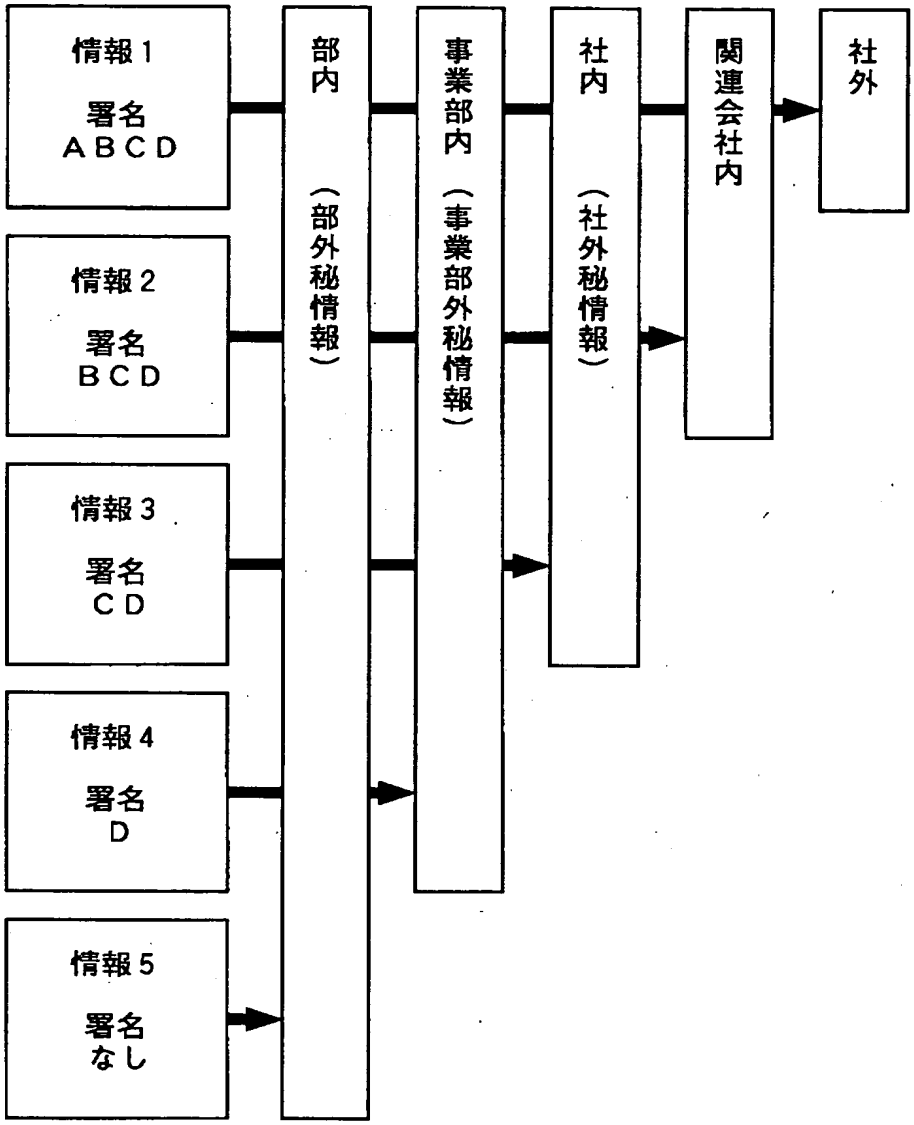
【図６】

図　6


1
11
社内 Network
10
8
3
WWW
Cache
WWW
Server
4
Internet
PC等
SW
WWW
Cache
8
WWW
Cache
8
8
WWW
Cache

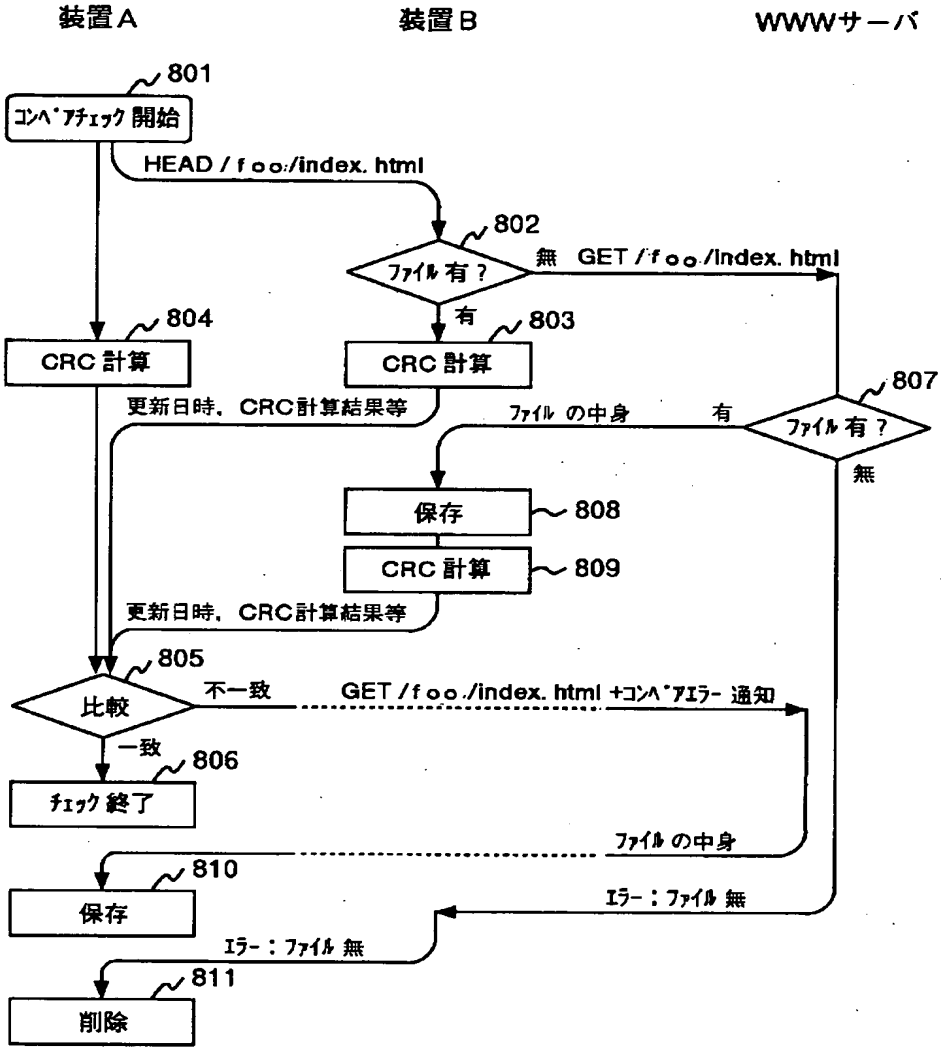
【図７】

図　７


情報１
署名
ＡＢＣＤ
情報２
署名
ＢＣＤ
情報３
署名
ＣＤ
情報４
署名
Ｄ
情報５
署名
なし
部内
（部外秘情報）
事業部内
（事業部外秘情報）
社内
（社外秘情報）
関連会社内
社外

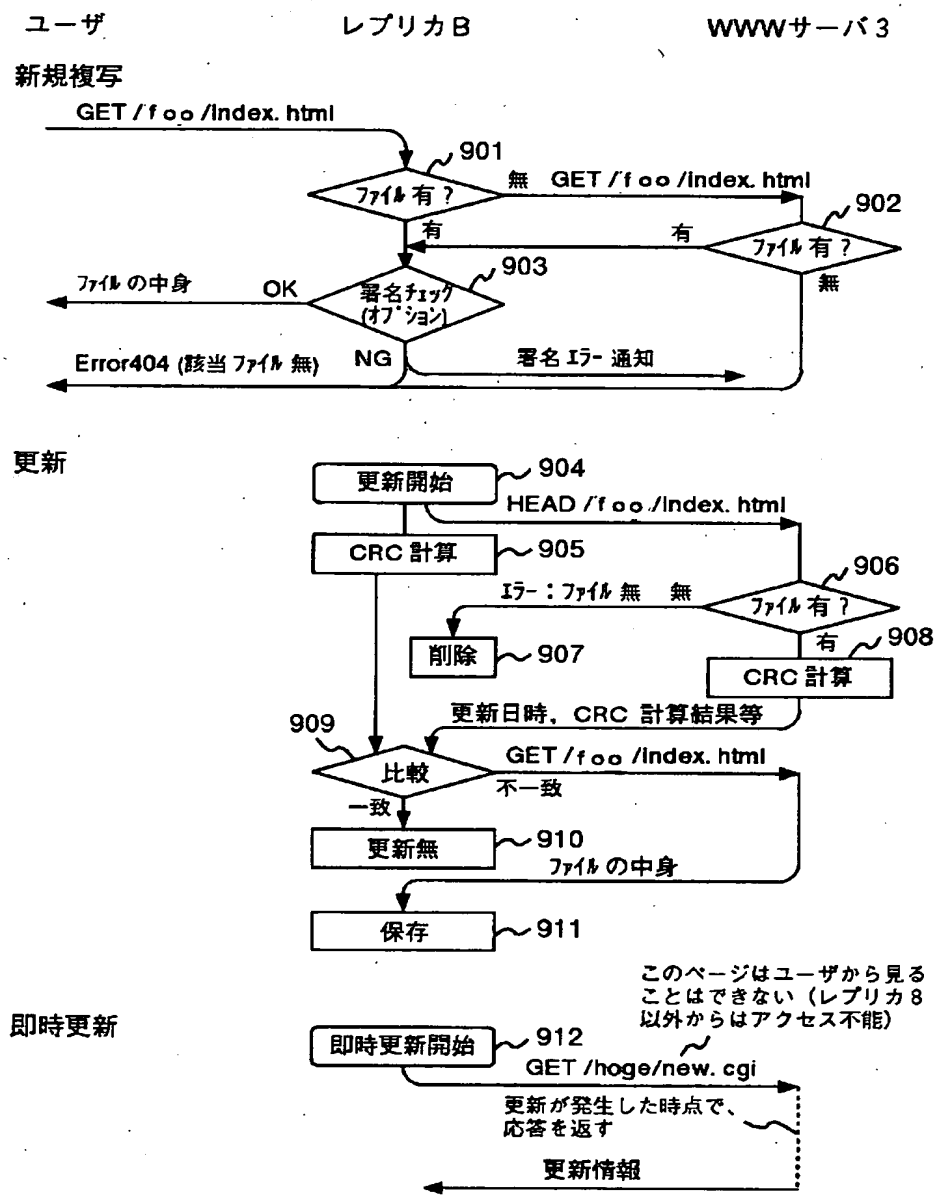
【図８】

図　8


装置A
装置B
WWWサーバ
801
ｺﾝﾍﾟｱﾁｪｯｸ 開始
HEAD / f o o /index. html
802
ﾌｧｲﾙ 有？
無
GET / f o o /index. html
有
804
CRC 計算
803
CRC 計算
807
更新日時，CRC計算結果等
ﾌｧｲﾙ の中身
有
ﾌｧｲﾙ 有？
無
保存
808
CRC 計算
809
更新日時，CRC計算結果等
805
比較
不一致
GET / f o o /index. html +ｺﾝﾍﾟｱｴﾗｰ 通知
一致
806
ﾁｪｯｸ 終了
ﾌｧｲﾙ の中身
810
保存
ｴﾗｰ：ﾌｧｲﾙ 無
ｴﾗｰ：ﾌｧｲﾙ 無
811
削除

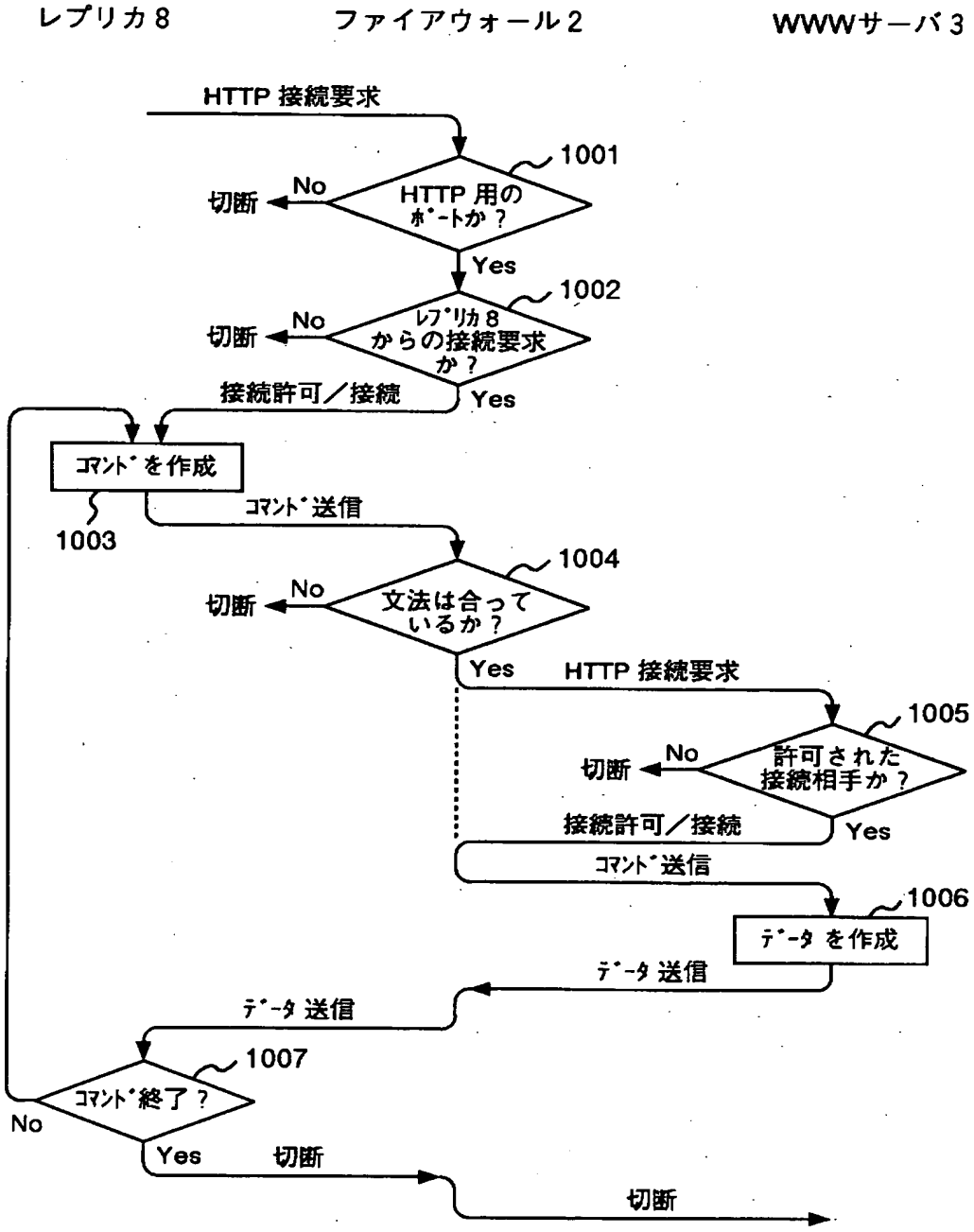
【図９】

図　9


ユーザ
レプリカB
WWWサーバ3
新規複写
GET /foo/index.html
901
ファイル有？
無
GET /foo/index.html
902
有
有
ファイル有？
903
ファイルの中身
OK
署名チェック
(オプション)
無
Error404 (該当ファイル無)
NG
署名エラー通知
更新
更新開始
904
HEAD /foo/index.html
CRC計算
905
906
エラー：ファイル無
無
ファイル有？
削除
907
有
908
CRC計算
更新日時，CRC計算結果等
909
比較
GET /foo/index.html
不一致
一致
更新無
910
ファイルの中身
保存
911
このページはユーザから見ることはできない（レプリカ8以外からはアクセス不能）
即時更新
即時更新開始
912
GET /hoge/new.cgi
更新が発生した時点で、応答を返す
更新情報

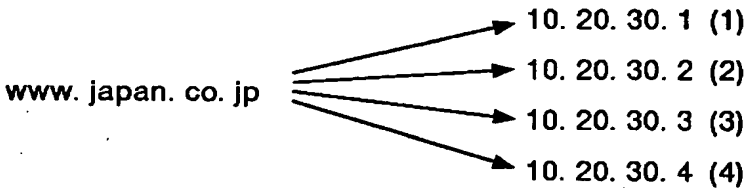
【図１０】

図　１０


レプリカ８
ファイアウォール２
WWWサーバ３
HTTP 接続要求
1001
HTTP 用の ﾎﾟｰﾄか？
No
切断
Yes
1002
ﾚﾌﾟﾘｶ８ からの接続要求か？
No
切断
接続許可／接続
Yes
ｺﾏﾝﾄﾞを作成
1003
ｺﾏﾝﾄﾞ送信
1004
文法は合っているか？
No
切断
Yes
HTTP 接続要求
1005
許可された接続相手か？
No
切断
接続許可／接続
Yes
ｺﾏﾝﾄﾞ送信
1006
ﾃﾞｰﾀを作成
ﾃﾞｰﾀ送信
ﾃﾞｰﾀ送信
1007
ｺﾏﾝﾄﾞ終了？
No
Yes
切断
切断

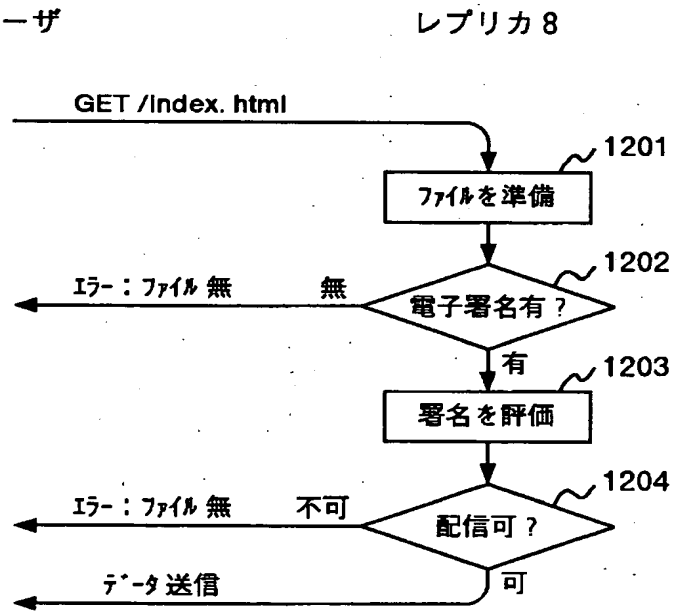
【図１１】

図　１１



【図１２】

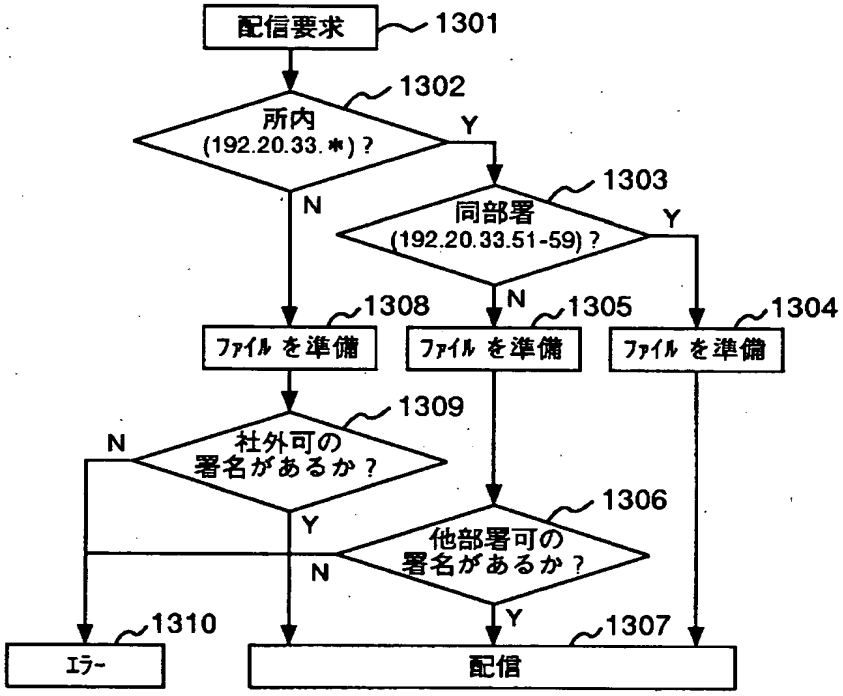
図　１２



【図１３】

図　１３

ユーザA (社外)	ユーザB (社内他部署)	ユーザC (社内同部署)
IP:172.16.199.201	IP:192.20.33.44	IP:192.20.33.56



【書類名】　要約書

【要約】

【課題】　インタネットに接続されていて不特定多数の利用者に情報を発信するコンピュータシステムにおいて、内外からの不正な侵入や改ざんからシステム全体を防護する簡便な方法がなかった。

【解決手段】　インタネットから見える装置は情報発信機器の複製のみとし、複製を複数設置することにより互いに比較させ改ざんを検出する。複製は電子署名の検査を実施し、不正であった場合は改ざんが発生したと見なし情報発信機器３から本来あるべき情報を再複製することもできる。情報発信機器はファイアウォール２により保護されているので、情報登録は容易に行うことができる。

【選択図】　図３

出　願　人　履　歴　情　報

識別番号　　〔０００００５１０８〕

１．変更年月日　　１９９０年　８月３１日
［変更理由］　新規登録
住　所　　東京都千代田区神田駿河台４丁目６番地
氏　名　　株式会社日立製作所